AFCEA-IO-3

4

NAVAL WAR COLLEGE
Newport, R.I.

INFORMATION OPERATIONS: A CONCEPTUAL PERSPECTIVE FOR STAFF ORGANIZATION AND FORCE EMPLOYMENT

By

Stephen G. Nitzschke
Cube # H-203A
LtCol USMC

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations Department.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

17 May 2005

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
17-05-05	FINAL	

4. TITLE AND SUBTITLE
Information Operations: A Conceptual Perspective for Staff Organization and Force Employment

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
LtCol. Stephen G. Nitzschke, USMC

Paper Advisor (if Any): LtCol. Derrill T. Goldizen

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Provost, Naval War College, for consideration in the Prize Essay Competition in the AFCEA category. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the

14. ABSTRACT

I

The JFC lacks an adequate information operations (IO) conceptual framework. Current definitions derived from various service perspectives have hampered his ability to effectively implement an IO strategy in an efficient manner. A different IO conceptual framework, when combine with appropriate definitions, will allow the JFC to more effectively and efficiently organize and employ forces to accomplish IO objectives. This paper suggests a different perspective that recognizes all military capabilities as potential contributors to an IO strategy, and recommends appropriate definitions to help redefine the traditional roles of the information operations and an information warfare officers.

15. SUBJECT TERMS
Information Operations, Information Domain, Information Warfare, JFIOCC, JIOTF, IO Cell, Decision Space, IO, IW.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		19	19b. TELEPHONE NUMBER *(include area code)* 252-675-2704

"Information operations are essential to achieving full spectrum dominance."

Joint Vision 2020

In military circles, there is no shortage of written documents outlining the important role information operations (IO) can play in achieving national security objectives. Joint Vision 2020 devotes 3 pages to the subject, claiming that "Improvements in doctrine, organization, and technology may lead to decisive outcomes resulting primarily from information operations."[1] Joint Publication 3-13 *Joint Doctrine for Information Operations* claims that if carefully conceived, coordinated and executed, IO can contribute to the combatant commander's efforts to defuse crises and return to peace. It may even help forestall or eliminate the need to employ military forces in combat situations.[2] These are bold claims considering there is still much disagreement among the services and within the joint community regarding the very nature of information operations.

In 1999, Air Force Captain John Shaw wrote in an article published by *Cyber Sword* that during two exercises with the United States Air Forces Europe (USAFE), "…the USAFE IO cell produced a wealth of IO plans and courses of action (COAs) at the component level. However, little centralized planning took place at the Joint or JTF level."[3] He listed two primary causes, (1) a lack of clear direction in doctrine or in practice, and (2) a lack in unity of command and no authoritative IO focal point or advocate.[4] Not surprisingly, Lieutenant Commander Anthony Clapp called IO's performance during OPERATION ALLIED FORCE, "lackluster," and blamed it on poor leadership and staff organization.[5]

In June 2001, Marine Corps Commandant General James L. Jones published ALMAR message 021/01. In that message he stated, "My goal is to operationalize [sic] IO in the

MAGTFS* within the next 18 months by leveraging existing joint doctrine, organizations and capabilities."[6] In 2003, Lieutenant Colonel David Pere served as the senior watch officer in the 1st Marine Expeditionary Force (I MEF) Command Operations Center (COC). He described his relationship with IO representatives during OPERATION IRAQI FREEDOM (OIF) as inconsequential to the overall fight. Today he believes IO is broken in the Marine Corps.[7]

These frustrations are merely symptoms of a larger issue. The joint force commander (JFC) lacks an adequate conceptual framework for information operations. Current definitions derived from various service perspectives have hampered the JFC's ability to effectively implement an IO strategy in an efficient manner. A different IO conceptual framework, when combined with appropriate definitions, will allow the JFC to more effectively and efficiently organize and employ his forces to accomplish IO objectives.

A Different Perspective

In 1997, Dr. Daniel Kuehl, a professor at the National Defense University wrote, "The greatest difficulty facing the development of IW [information warfare] today is not technological but conceptual, because there is no common understanding or acceptance of what constitutes IW."[8] Joint doctrine describes IW as a subset of IO. It is information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.[9] Joint Vision 2020 contains a section on IO outlining the multidimensional definition and meaning of "information." It may be viewed as a target, a weapon, a resource and/or a domain of operations: "Our understanding of the interrelationships of these variables and their impact on military operations will determine the nature of information operations in 2020."[10] At present our understanding of these relationships is not monolithic.

---

* Marine Air Ground Task Forces

In reality, information operations have occurred for centuries, long before Samuel Morse invented the telegraph. Professor Kuehl provides the following example:

> Indeed, one could argue that the stone carvings that Assyrian rulers made of conquered peoples and cities being enslaved and pillaged were intended as much to cow and terrify current and potential subjects as to inform archeologists thousands of years later about what hard and cruel people they were.[11]

The Assyrians, however, utilized much more than just stone and chisel to shape the information environment. A. K. Grayson says that the chief occupation of the Assyrian king and state was warfare. Their primary weapons were the spear, bow, sling, dagger, sword, mace, and battle-axe.[12] In the ninth century B.C. the Assyrians embarked on annual campaigns to conquer cities and peoples throughout modern day Iraq, Syria and Israel. Although siege warfare was a common practice, the Assyrians realized this war form could become a long and costly affair. Their preferred method was psychological, and a variety of tactics were employed. At first high-ranking officers would stand outside city walls and offer reasonable arguments that might compel the inhabitants to disobey their rulers and open the gates.

If their arguments where rebuffed, the Assyrians would target a specific group or city for destruction. Once defeated, they would horribly mutilate the population, burn homes and appropriate their belongings. "The skins of flayed people were prominently displayed and corpses erected on stakes on the spot as testimony to what the Assyrians could do."[13] Grayson claims this "calculated frightfulness" or psychological warfare was supremely successful: "…once they heard of these acts, [the population] commonly surrendered to the Assyrian army without further resistance; indeed there were campaigns which met no hostilities, so widely had Assyrian terror spread."[14] Grayson makes one final important point, "…the terror was selective. While the Assyrian king boasts of wholesale slaughter and devastation, in practice only certain pockets of resistance were subjected to this treatment."[15]

Physical attack as an IO capability is the subject of much debate. Vice Admiral Arthur Cebrowski said while President of the Naval War College, "Warfare is intended not to kill someone, but to change their behavior. If you kill someone you dramatically change their behavior."[16] Joint publication 3-13 mentions physical attack/destruction as a major capability to achieve IO objectives, but current service and joint initiatives list physical attack as a supporting or related activity. Air Force doctrine does not include physical attack in its list of IO capabilities.[17] The Army's Field Manual (FM) 3-13 *Information Operations* recognizes the Department of Defense (DoD) definition for information operations as the employment of five core capabilities: electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), operations security (OPSEC), and military deception (MILDEC). Not one of these core capabilities possesses a lethal component.[†] Indeed the prevailing consensus is to use IO in lieu of physical force. This construct has benefited some traditionally neglected warfare specialties, but it has not improved the commander's ability to effectively focus IO efforts. The JFC requires a conceptual framework that recognizes all military actions as potential contributors to his IO objectives, both lethal and non-lethal.

As professor Kuehl points out, most service perspectives rely on some concept of the information environment, defined in joint doctrine as, "The aggregate of individuals, organizations and systems that collect, process, or disseminate information; also included is the information itself."[18] Using this definition as a starting point, individual services have attempted to "carve-up" this space to suit their particular operational concepts and resource requirements. The Air Force divides the information environment into three domains: the physical, cognitive and information domains.[19] FM 3-13 acknowledges that friendly, adversary, and other personnel

[†] The one possible exception is the high speed anti-radiation missile (HARM) used by aircraft conducting EW missions to suppress enemy air defense radars.

who make decisions and handle information are a part of the information environment. However, it specifically excludes the surrounding physical realm and actions that affect the information environment. "Climate, terrain, and weapons effects (such as electromagnetic pulse or blackout) affect the information environment but they are not part of it."[20]

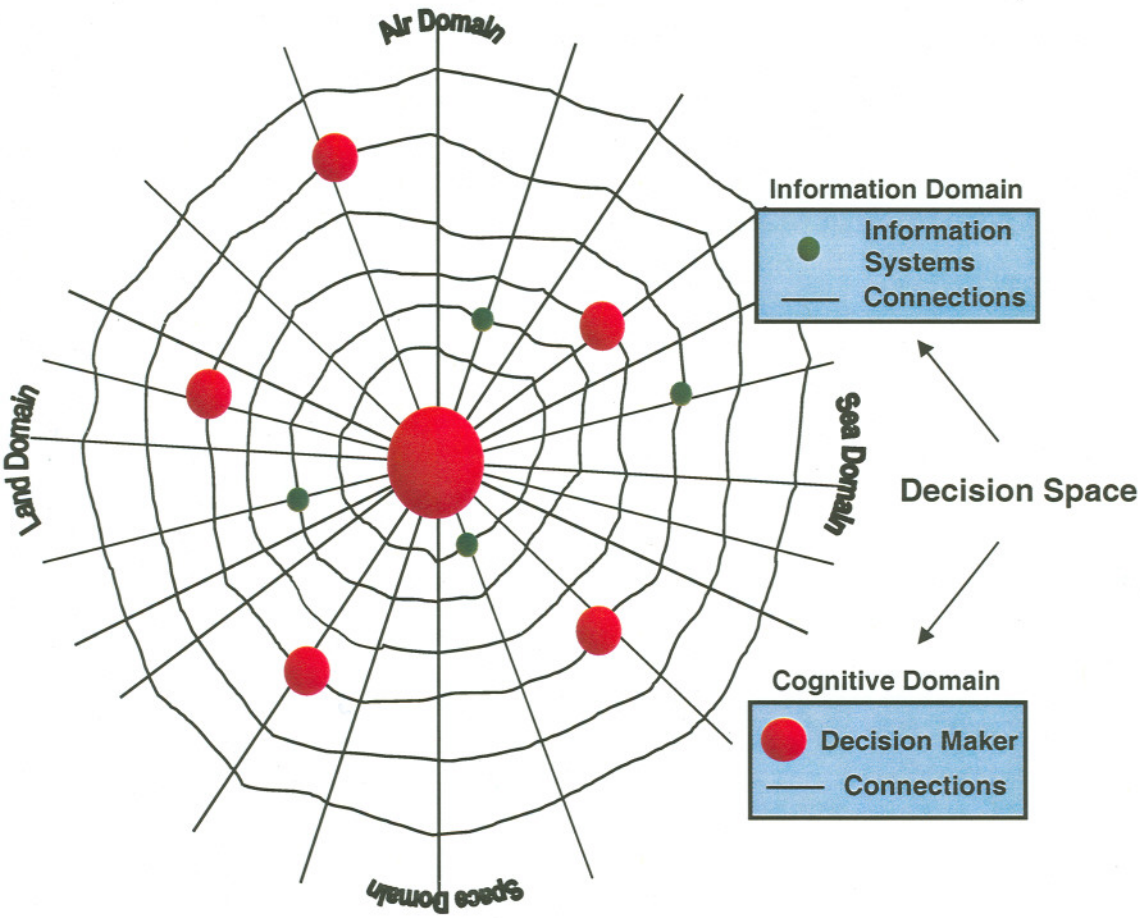
Rather than visualize the information environment from the outside looking in, it might be helpful to begin with the decision maker himself, the joint force commander (JFC), and view the information environment from the inside looking out. The JFC's view is one of almost endless possibilities. Herbert A. Simon says that "people solve problems by [a] selective, heuristic search through large problem spaces and large data bases."[21] This large data base we can refer to as the *information realm;* it includes the battlespace in its entirety.

Yet, only a fraction of the potential available data can ever be adequately processed. Even this data is constrained by the limits of human capacities. The JFC is constantly faced with the reality of making decisions based on a limited knowledge of the information realm.

> These limits are imposed by the complexity of the world in which we live, the incompleteness and inadequacy of human knowledge, the inconsistencies of individual preference and belief, the conflicts of value among people and groups of people, and the inadequacy of the computations we can carry out, even with the aid of the most powerful computers...we must simplify our problem formulations drastically, even leaving out much or most of what is potentially relevant."[22]

This limited information resides in what we will call the *decision space*, a subset of the information realm. The decision space is composed of human decision makers, information and information systems. Information and information systems fall within the information domain, while human decision makers have an exclusive place reserved in the cognitive domain. Connections between (and within) domains form networks spanning the entire battlespace. Network architecture (connectivity), its capacity, and its quality are part of the decision making

process. This process has a significant impact on the difference between what is available in the information realm, and what is actually used within the decision space (See Figure 1.).



Information Realm
Figure 1.

The JFC selects and interprets data from the information realm through a cognitive and/or automated process that blends information and insight. The result is a cognitive model[‡] of the information realm upon which decisions are based. The commander's battlefield area evaluation is an interpretation of the information realm as seen through the lens of his own personal political, military and social experiences, a modified and much reduced version of the aggregated

[‡] A mental picture or pictures of the battlespace based on information and insight. Its formulation can involve interpretation, intuition and prediction.

whole. Military commanders particularly adept at evaluating these incomplete models, and acting appropriately, possess a measure of that gift Carl Von Clausewitz refers to in the French expression *Coup D'oeil.*

A commander's cognitive model of the information realm cannot discount, as FM 3-13 might suggest, the physical environment. Terrain, weather and weapons effects all convey information through the cognitive interpretation of a decision maker. The advent of bad weather on June 4th 1944 caused General Dwight D. Eisenhower to postpone OPERATION OVERLORD for 24 hours. On June 5th chief SHAEF[§] meteorologist, Group Captain J.M. Stagg, predicted the weather would clear just long enough to conduct the D-Day landings on the 6th. Eisenhower rescheduled the landings based on his confidence in Stagg's information. In contrast, German meteorologists came to a different conclusion, and Rommel went home to Germany for his wife's birthday.[23]

A chemical warhead is not designed to transmit information, but awareness of its possession provides information nonetheless. Indeed, a commander may choose a particular course of action simply because his cognitive model contains insight into a particular threat. During the 1991 Persian Gulf War, coalition forces were ordered to begin the ground offensive in chemical protective suits because General Schwarzkopf believed Saddam Hussein possessed and would use chemical weapons.

By the same token, awareness of friendly weapons effects may contribute to an adversary's cognitive model. A commander's decision to shoot rather than detain looters during post hostilities can shape an adversary's decision space, creating specific behaviors. Force deployments are sometimes designed for this very purpose. In 2003 the United States openly deployed EA-6B Prowlers and F-117 stealth fighters to the Pacific theater, sending information

[§] Supreme Headquarters Allied Expeditionary Force

that America could respond to aggression on the Korean peninsula while simultaneously fighting a war in the Persian Gulf. The U.S. military withdrawals from Beirut in 1983 and Somalia in 1995 contributed to the information realm. The question of whether Al Qaeda recognized these withdrawals within their decision space is an on-going debate. Osama Bin Laden's declaration that America is a "paper tiger" offers some evidence to suggest they did.

Cognitive connections formed through cultural, religious or political networks can also influence the decision space. A human network composed of individuals sharing a common understanding serve to reinforce or augment cognitive models. Military commanders use human connections for IO activities that augment an adversary's battle field perceptions. Recall the Assyrian kings, whose mere reputation caused entire cities to surrender without a fight.

Ho Chi Minh and Vo Nguyen Giap relied on the Vietcong infrastructure (VCI), a human network, to implement a strategy Douglas Pike refers to as *dau tranh*. Literally translated, *dau tranh* means "struggle." It consisted of two elements, *dau tranh vu trang* (armed struggle) and *dau tranh chinh tri* (political struggle). Both elements employed violence to achieve their objectives. And much like the Assyrians, "the Vietnamese communists erased entirely the line between military and civilian by ruling out the notion of noncombatant."[24] While a regular North Vietnamese army fought an armed struggle, irregular forces formed a human network of *dich van*, *binh van* and *dan van* cadres that managed the political struggle. These cadres employed activities and programs involving motivation, social organization, communication of ideas and mobilization of manpower and support. Pike states the following:

> Organization is the great god of *dau tranh* strategy. It counts for more than ideology or military tactics. The basic instrument of a united front, an organization of organizations, casting a web over the people, enmeshing them.... *Dau tranh* strategy engenders a war of competing systems and organizations.[25]

Interestingly, professor Kuehl portrays IW and IO in similar fashion by describing both as "the struggle to control and exploit the information environment."[26] The North Vietnamese example highlights the cognitive aspect of that struggle.

The cognitive domain is only one component of the decision space. The information domain is its second component. The information domain is composed of information and information systems used to augment, alter or corrupt the cognitive model. Facts, data, or instructions qualify as information. Information systems collect, process, and/or disseminate information using connections. In addition to human connections, technological networks offer physical connections that can increase a JFC's decision space or destroy an adversary's.

Some systems even make decisions for the commander. The automated engagement feature in a Patriot missile battery is but one example. In this instance the physical system forms a mathematical rather than cognitive model of the information realm. This model is a function of selected variables and their particular combinations, chosen of course by a human programmer.

The rapid growth of information technology (IT) has increased the information domain's value as a warfare specialty to the JFC. During the Civil War, Ulysses S. Grant could rely on a telegraph network to communicate with General Halleck in Washington and his subordinate commanders in the field. Admiral Nimitz could rely on radio networks to accomplish similar tasks during World War II. Today commanders employ netted digital communications and computers to simultaneously collect and disseminate information about the battlespace. The global command and control system (GCCS), blue force tracker (BFT) and link monitoring system (Link 16) are a few among many examples.

Neither the cognitive nor the information domain is distinctly separate from the air, land, sea, or space domains. Physical and cognitive connections collect, process, and/or disseminate

information among decision makers in every domain. Like *dau tranh's* political cadres, the information and cognitive domains represent systems within a system. And like the VCI, their architecture can extend well beyond military circles (see figure 1).

The confusion today is caused by what Dr. Kuehl refers to as "the marriage of computers and telecommunications" and "global omni-linking."[27] These phenomena have increased the number of individuals, organizations and systems that have the access and capability to add to the information realm. In 1959 there were 5000 stand alone computers, no FAX machines and no cellular telephones. Electronic mail (e-mail) did not exist. In 1999 there were 180 million computers, 14 million FAX machines, and 40 million cellular telephones. Today e-mail is more often used than the postal service.[28] The JFC today must often consider non-military individuals and organizations that, through the power of modern IT, can shape his decision space. In July 1995, Julio Cesar Ardita, a 21-year-old student at the University of Argentina, broke into the U.S. Naval Command, Control, and Ocean Surveillance Center's computer system and installed software that allowed him to alter or destroy network files, or make them inaccessible to legitimate users.[29] On a greater scale than ever before, these connections, and their resulting networks, have blurred the lines between civilian and military, combatant and non-combatant, public and private, even between war and peace.

Modern information technology has increasingly obscured the distinction between strategic, operational and tactical levels of war; between higher, adjacent, and subordinate levels of command; and most relevant to the JFC, between individual staff functions. As professor Kuehl states, "Warriors seek to distinguish between different kinds of operations so that they can establish clear lines of authority and control. Unfortunately, this may not be fully possible in the information battlespace."[30] During OPERATION IRAQI FREEDOM the combatant commander

initially identified 21 IO objectives and 94 separate measurable tasks to achieve them. Of those tasks, 29 were assigned to CENTCOM headquarters, 25 to the Combined Forces Air Component Commander (CFACC), 11 to the Combined Forces Land Component Commander (CFLCC), 7 to the State Department, and 7 to the Joint Psychological Operations Task Force (JPOTF). Not a single IO task was assigned to an IO officer, IO cell, IO task force or IO component commander. Forty-seven tasks did not even involve IO core capabilities as currently defined.[31]

Before specifically addressing IO staff organization and force employment, it is first necessary to develop a few new definitions. These definitions emphasize the limited capacity decision makers possess to interpret an aggregate, complex information realm. To cope with complexity, decision makers utilize the cognitive and information domains to construct models within their unique decision space, simplifying the problem by reducing the available data to a manageable level. Because the cognitive and information domains span the entire battlespace, the JFC must have all his forces available to achieve IO objectives. This perspective recognizes a difference between the information realm and the unique decision spaces of both friendly and adversary forces. Information operations focus primarily on shaping the decision space to aid friendly forces, and hinder an adversary.

New Definitions

Many military professionals are tired of arguing over definitions, but a lack of agreement on the nature of information operations has a significant impact on staff organization and force employment. "Definitions are everything,"[32] says retired Navy Captain Scott Rome, a former cryptologist who has developed IO policy in Washington and IO procedures for both the Second and Seventh Fleets. Although the Department of Defense issued an IO Roadmap in October

2003, it has yet to publish a much anticipated rewrite of the instruction that defines IO for the individual services.**

The current and most enduring definition is found in joint doctrine: "Actions taken to affect adversary information and information systems, while defending one's own information and information systems."[33] FM 3-13 defines IO as the integrated employment of the five core capabilities "in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision making."[34] The Air Force defines IO as "the integrated employment of the capabilities of influence operations, electronic operations, and network warfare operations in concert with specified integrated control enablers, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."[35] The Navy has made information operations a "warfare area" that consists of the five core capabilities, supported by physical destruction, intelligence, public affairs (PA), and civil affairs (CA).[36] The Marine Corps has no doctrinal definition for information operations. Its efforts to view the discipline as an integrating enabler for other battlespace functions was cut short by the DoD initiative to redefine IO as a core competency that could perform both supported and supporting roles in military operations.

Not surprisingly, the current rewrite of joint publication 3-13 has, for the moment, abandoned a definition for IO in favor of a description involving an amalgam of service perspectives.[37] The latest draft publication has generated over 390 pages of comments and suggested changes from the warfighting community--an unprecedented amount for a second draft, according to James Seerden, head of the Joint Doctrine Division at the Navy's Warfare Development Command.[38]

** Captain Rome suggests the new DOD IO instruction 3600 has been delayed because of the resource and funding implications that accompany such a document.

Nevertheless, armed with the previously outlined conceptual framework, it is possible to suggest key definitions that may improve joint force organization and employment.

Information Realm: ***The aggregate interaction between individuals, organizations and systems within the physical battlespace and cognitive domain.*** The physical battlespace includes all battlespace domains, including the information domain. "Systems" also includes ecological, geological and meteorological systems from the physical environment. In effect, the information realm represents the absolute truth, the totality of all available information, correctly identified and uniformly processed and interpreted. It symbolizes a theoretical reality that Herbert Simon might describe as one of mathematical predictability or, "a world in which the probability distributions of all relevant variables can be provided by the decision makers."[39] He compares this world to the macroscopic behavior of an ideal gas. A military professional might recognize this realm as akin to Clausewitz's environment for theoretical war. The same fog and friction that limits Clausewitz's theoretical concept also affects the information realm. Thus, the need for a definition that accounts for such factors.

Decision Space: ***That portion of the information realm used to make decisions. It consists of human decision makers, information, and information systems that blend information with insight.*** Networks are a key feature of the decision space. Network connections, whether physical or cognitive, provide a resource for, or may become a target of, the joint force. The insight derived from purely automated information systems is gained only as a consequence of the variables and related mathematical equations chosen by the human programmer. The human decision maker has the option of completely automating decision-making, making a purely cognitive choice, or combining personal insight and information through some analytical or cognitive process. In any case, a decision is made based on a limited

decision space that contains connections and reflects the decision maker's personal values, beliefs and predilections.

Military Information Operations (IO): Military actions, activities and/or operations specifically synchronized and integrated to shape the decision space. All military actions contribute to the information realm. Military information operations specifically target the decision space to gain some advantage over an opponent. Defensive IO focuses on protecting the friendly decision space. Offensive IO focuses on attacking the enemy's. Information operations in general include activities in both the information and cognitive domains. Therefore, understanding a decision maker's cultural, political, and military beliefs is just as important as knowing the systems and connections (networks) used to augment, alter or corrupt those beliefs.

Information Domain: That portion of the battlespace containing information, information systems, and information networks designed to collect, process, or disseminate information; also included is the information itself. This definition is necessary to make a clear distinction between the physical systems and connections (links) used to process information, and the cognitive domain, which involves interpretation, intuition and prediction. Computer hardware and software, fiber optics, telecommunications devices and the information they collect, process, and disseminate are a part of this domain. In this manner cyberspace (and other information related systems) occupies a "place" conceptually useful to the JFC.

Military Information Warfare (IW): Military actions, activities and/or operations using information, information systems and information networks specifically integrated to affect the information domain. This definition restricts information warfare to the physical world of telecommunications, global omni-linked systems, computers, the cyber world… It

therefore deals with the physicality of the decision space. The target of an "information warrior" is the information domain, not its cognitive counterpart. He attacks or defends the functional aspects of information systems and/or its resident information. His activities may not directly accomplish a stated IO objective. For example, IW can support command and control by providing computer security services or enhance intelligence assessments by monitoring foreign IT activities.

Organization and Force Employment

It is certainly possible to quibble with the previous definitions. For instance, one might argue that a bicycle messenger, delivering a letter he cannot access, is part of the information domain. The same might be said of a radio announcer directed to broadcast a message he did not craft. This particular construct places humans in the cognitive domain because they possess the ability to make cognitive choices. The bicycle messenger and radio announcer may choose not to deliver a message or make an announcement. In any event, these definitions were derived primarily for their organizational and employment implications.

The IO perspective outlined in this paper, coupled with new definitions, provide the JFC with a conceptual framework to more efficiently and effectively employ his forces to achieve IO objectives. Effectiveness is derived from the recognition that IO is not restricted to five core capabilities and variously defined related and supporting activities. It involves integrating any or all force capabilities, to specifically influence the decision space. Efficiency is gained by focusing IO efforts only on relevant portions of the information realm. Additional efficiencies are realized by organizing staff functions and warfare specialties to reflect this conceptual framework.

It should be obvious by now that the commander himself is the ultimate information operations officer. The JFC is the only individual with the access and authority to integrate and synchronize all military actions, activities and operations. He is also responsible for evaluating how military operations will affect the enemy and other theater and strategic organizations tasked with achieving national security objectives. Today this not only includes joint and coalition military partners, but interagency organizations and private institutions. A career IO force must contain leaders capable of assisting the commander in this endeavor. An IO officer must recommend and evaluate joint force operations to shape the decision space (both information and cognitive domains).

In current doctrine the IO officer plays an often redundant role on the commander's staff, performing duties traditionally assigned to the operations officer. He has little authority and almost no credibility. Joint and service publications describe the IO officer as a "coordinator" or "the central point of contact." Significant warfare specialties within the IO cell have much more credibility and influence. Some staff organizations include a Joint Psychological Operations Task Force (JPOTF) that deals directly with the JFC, as was the case during OPERATION ALLIED FORCE in 1999. The Air Force disperses IO representatives from the Information Warfare Flight (IWF) among the various divisions of its Air Operations Center (AOC), but it consolidates electronic warfare operations into a single electronic warfare coordination cell (EWCC). "When military activities appear likely and crisis action planning commences, the COMAFFOR's[††] EWCC should be established to directly plan and coordinate with the JFC and component staffs to ensure integration of EW in the overall campaign plan."[40] In such cases the IO representative is subordinated to, by becoming a member of, the EWCC.

[††] Commander, Air Force Forces

Information operations as a core competency may involve any or all of the commander's capabilities. This is a key insight that helps define a new role for the IO officer as a special advisor to the JFC. In this capacity, the IO officer acts much like the legal officer, chaplain or sergeant major, gaining credibility and influence from his special relationship to the commander. His role subsumes the duties of an effects assessment officer by assigning him the responsibility of interpreting and predicting how military activities might affect the decision space of both friendly and enemy forces.

This is a tall order. It requires an education and experience level far beyond that defined in current IO job descriptions. It involves assessing human nature, integrating military capabilities and evaluating their resulting interactions. Ideally the IO officer is well versed in the cultural, religious, linguistic, and social characteristics of the battlespace environment. He has a grasp of military history and understands systems and networks (human and automated). He is an intelligence officer and an operations officer.

The information warfare officer (IWO), on the other hand, is purely a technical expert capable of waging war exclusively within the information domain. His particular specialty is computer network operations (CNO). Like the fighter pilot using an aircraft to gain air superiority, or the navy commander using a submarine to gain control of the sea, the "information warrior" uses a computer to dominate the cyber world. His actions, activities, and operations may support other military capabilities such as psychological operations or physical destruction, or they may provide support to command and control, logistics or deception operations.

Should the information operations cell then be a thing of the past? The IO cell in joint publication 3-13 provided a way for non-kinetic, non-lethal battlespace capabilities to gain

greater visibility in the targeting and staff planning process. This visibility presumably increased their utility and synergy. A draft copy of this document today only adds more capabilities and activities.[‡‡] It does not change the ineffective role an IO officer has traditionally played on the joint staff.

An IO cell still may be necessary, if the commander's IO objectives require more non-traditional capabilities, or if the operations officer is incapable of integrating such a diverse array of activities. In most cases, especially at the JTF level and below, commanders lack the infrastructure and time to support large staffs and fight pitched battles at the same time. A smaller cell, tailored for specific needs and led by the IO officer might include a cultural expert, a linguist and/or a computer specialist. The cell may expand or contract depending on the mission objectives and the commander's priorities. The key is to construct a cell capable of advising the JFC on integrating military forces to affect the decision space; much like the JFACC advises the JFC on matters concerning air space or the JFMCC on sea space.

Others have argued for a Joint Force Information Operations Component Commander (JFIOCC), or a Joint Information Operations Task Force (JIOTF), modeled after the JPOTF example. These efforts have fallen flat simply because the assets and organizations a JFIOCC or JIOTF must task traditionally fall under other functional and/or component commanders. An effective IO commander within the joint force, in any form, would require significant organizational restructuring, adding to an already bloated staff structure. Additionally, establishing a separate functional IO command effectively stovepipes or segregates a capability whose vary nature requires integration, coordination and synchronization. This is the case with

[‡‡] The draft version of JP 3-13 on page IV-6 depicts a proposed IO cell. It adds the chaplain, a liaison officer from STRATCOM, and a physical security and state department representative to the original version depicted on page IV-3 of the current document.

current IO core capabilities where the commander has come to view IO as primarily a non-lethal, non-kinetic activity.

Conclusion…

The JFC lacks an adequate IO conceptual framework. Current definitions derived from various service perspectives have hampered his ability to effectively implement an IO strategy in an efficient manner. The new conceptual framework outlined in this paper improves effectiveness by allowing the JFC to employ any military activity or capability in an IO strategy specifically focused on the unique decision space of friendly and adversary forces. Efficiency is obtained through a staff organization that reflects this reality. The IO officer becomes a special advisor to the commanding officer, with expertise in integrating military actions and activities to shape the decision space. His staff is augmented based on JFC mission objectives and associated priorities. The IW officer is a warfare specialist capable of fighting in the information domain. He can function within an IO cell or support other battlespace activities as a member of the operations staff.

Like the ninth century B.C. Assyrian king who employed stone and chisel along with the battle axe, today's joint force commander must employ the right combination of the modern day equivalent. This conceptual perspective, combined with their associated definitions and organizational options, will permit the JFC to more efficiently and effectively obtain his IO objectives.

-End Notes-

[1] Joint Chiefs of Staff, *Joint Vision 2020* (Washington, DC: June 2000), 30.
[2] Joint Chiefs of Staff, *Joint Doctrine for Information Operations,* Joint Pub 3-13 (Washington, DC: 9 Oct 98), I-19
[3] John Shaw, *Does the JFC Need a JIOTF? Strengthening IO Doctrine,* Cyber Sword, (Fall 1999): 4.
[4] Ibid.
[5] Anthony J. Clapp, *Information Operations and Joint Vision 2020: Ready to Accept the Challenge*, (unpublished research paper, U.S. Naval War College, Newport, RI: 2002) 9.
[6] Headquarters, United States Marine Corps, ALMAR 021/01 (DTG 051600Z JUN 01), 2.
[7] Lieutenant Colonel David Pere, Branch Head for Command and Command Support, Marine Corps Combat Development Command. Telephone interview by author, 21 April 2005.
[8] Daniel Kuehl, *Defining Information Power*, Strategic Forum Paper #115 (National Defense University, June 1997), On-line at <http://ndu.edu/inss/strforum/SF115/forum115.html/> [20 Apr 2005], 2.
[9] Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Pub 1-02 (Washington, DC: 12 Apr 2001 as amended through 30 Nov 2004), 257.
[10] JV 2020., 29
[11] Daniel Kuehl, *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*. In Computer Network Attack and International Law, ed. Michael N. Schmitt & Brian T. O'Donnell, Vol. 76, 35-58. (Newport RI: Naval War College 2002), 38.
[12] A.K. Grayson, *Assyrian Civilization*, The Cambridge Ancient History Vol III, Part 2, ed, John Boardman, I.E.S. Edwards, N.G.L. Hammond, and E. Sollberger, (New York: Cambridge University Press, 1991) 221.
[13] Ibid
[14] Ibid.
[15] Ibid.
[16] Arthur Cebrowski, as quoted by the College of Aerospace Doctrine, Research and Education, in *The Information Operations Environment IW-200*, power point brief, 20 Apr 2005. on-line at
< http://www.iwar.org.uk/iwar/resources/iw-course/iw-200%20Define%Envir.ppt > [20 Apr 2005]
[17] United States Air Force, *Information Operations*, AFDD 2-5 (Montgomery, AL: 11 Jan 2005), 7.
[18] JP 1-02. 265.
[19] AFDD 2-5. 3.
[20] United States Army, *Information Operations: Doctrine, Tactics, Techniques and Procedures*, FM 3-13 (Washington, DC: November 2003), 1-2.
[21] Herbert A. Simon, *Decision Making and Problem Solving*, Report of the Research Briefing Panel on Decision Making and Problem Solving 1986, by the National Academy of Sciences (Washington DC: 1986) as found on-line at < http://www.dieoff.org/page163.htm > [29 April 2005], 2.
[22] Ibid.
[23] Carlo D'Este, Speech to the Eisenhower Institute, 29 April 2004. On-line at
< http://www.eisenhowerinstitute.org/presscenter/DESTETranscript.htm > [6 May 2005]
[24] Douglas Pike, PAVN: People Army of Vietnam, (Novato, CA: Presidio Press, 1986) 260.
[25] Ibid. 263.
[26] Daniel Kuehl, *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*. In Computer Network Attack and International Law, ed. Michael N. Schmitt & Brian T. O'Donnell, Vol. 76, pg. 35-58. (Newport RI: Naval War College 2002), 37.
[27] Daniel Kuehl, *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*. In Computer Network Attack and International Law, ed. Michael N. Schmitt & Brian T. O'Donnell, Vol. 76, 35-58. (Newport RI: Naval War College 2002), 39.
[28] *The Information Operations Environment IW-200*, College of Aerospace Doctrine, Research and Education: power point brief, 20 Apr 2005. on-line at
< http://www.iwar.org.uk/iwar/resources/iw-course/iw-200%20Define%Envir.ppt > [20 Apr 2005]
[29] Department of Commerce, National Oceanic & Atmospheric Administration-Western Administrative Support Center website. On-line at <http://www.wasc.noaa.gov/wrso/security_guide/hacking.htm > [16 May 2005]

[30] Daniel Kuehl, *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*. In Computer Network Attack and International Law, ed. Michael N. Schmitt & Brian T. O'Donnell, Vol. 76, pg. 35-58. (Newport RI: Naval War College 2002), 45.
[31] Naval War College, Joint Military Operations Department, *ISR and Information Operations in Iraqi Freedom-2003*, (Newport, RI: 19 Aug 2004), 55-59.
[32] Scott Rome, USN (Ret.) Navy Warfare Development Command (NWDC), interview by author, 26 April 2005. Newport RI.
[33] JP 1-02. 256.
[34] United States Army, *Information Operations: Doctrine, Tactics, Techniques and Procedures*, FM 3-13 (Washington, DC: November 2003), iii.
[35] AFDD 2-5. 1.
[36] United States Navy, *Navy Information Operations*, NWP 3-13 (Newport, RI; Jun 2003), 1-2.
[37] Joint Chiefs of Staff, *Joint Doctrine for Information Operations,* Joint Pub 3-13 (Washington, DC: 9 Oct 98), I-1
[38] James Seerden, Director, Joint Doctrine Division, Navy Warfare Development Command, interview by author, 6 April 2005. Newport, RI.
[39] Herbert A. Simon, *Decision Making and Problem Solving*, Report of the Research Briefing Panel on Decision Making and Problem Solving 1986, by the National Academy of Sciences (Washington DC: 1986) as found on-line at < http://www.dieoff.org/page163.htm > [29 April 2005], 2.
[40] AFDD 2-5. 35.

Bibliography

Bloom, Bradley. "Information Operations in Support of Special Operations," Military Review. (Jan/Feb 2004): Vol. 84, Iss. 1; pg. 45.

Bowman, Paul. "Information Operations: Strategy or Mission? Reflections on Allied Force." Cyber Sword, (Summer 2001): Vol. 4, no. 1, p. 19-22.

David, John D. "Leading the Information War," Marine Corps Gazette, (Feb 2005): Vol. 89, Iss. 2; pg. 24-25.

Department of Defense. Information Operations Roadmap, Washington, DC; October 2003.

Dowell, Cody D. Romanych, Marc J, & Carter, Jerry M. "Joint Task Force Information Operations," Cyber Sword, (Fall 1999): Vol. 3, Iss. 1. pg. 6.

Department of the Air Force. Basic Air Force Doctrine. Air Force Doctrine Document 1 Headquarters, Air Force Doctrine Center, Montgomery AL: 17 Nov 2003.

Department of the Air Force. Information Operations. Air Force Doctrine Document 2-5 Headquarters, Air Force Doctrine Center, Montgomery AL: 11 Jan 2005.

Department of the Army, Information Operations: Doctrine, Tactics, Techniques and Procedures, Field Manual 3-13, Washington, DC: 28 Nov 2003.

Department of the Navy. Navy Information Operations. Naval Warfare Publication 3-13. Naval Warfare Development Command, Newport RI: June 2003.

Emery, Norman. "Information Operations in Iraq." Military Review. Fort Leavenworth: (May/Jun 2004): Vol. 84, Iss. 3. pg 11.

Grayson A.K. "Assyrian Civilization." In The Cambridge Ancient History: The Assyrian and Babylonian Empires and Other States of the Near East, from the Eighth to the Sixth Centuries B.C., edited by John Boardman, I.E.S. Edwards, N.G.L. Hammond, and E. Sollberger, Vol III, Part 2. pg. 194-227. New York: Cambridge University Press, 1991.

Hanson, Lynn. "Organization of the Information Operations Cell for a Joint Task Force." Cyber Sword, (Spring 2000): Vol. 4, no. 1, pg. 29-31.

Hubbard, Zachary P. "IO in the Information Age." Journal of Electronic Defense. (Apr 2004): Vol. 27, Iss. 4; pg. 51.

Josten, Richard J. "IO Support to the CINC." Cyber Sword, (Fall 1999): Vol. 3, no. 1, pg. 10-13.

Krumm, Kenneth & Romanych Marc J. "Tactical Information Operations in Kosovo." Military Review, (Sep/Oct 2004): Vol. 84, Iss. 5; pg 56.

Kuehl, Daniel Dr. "Defining Information Power." National Defense University, Strategic Forum Paper No#115 Jun 1997 on-line at <http://ndu.edu/inss/strforum/SF115/forum115.html/ > [20 Apr 2005]

Kuehl, Daniel Dr. "Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age." In Computer Network Attack and International Law, edited by Michael N. Schmitt & Brian T. O'Donnell, Vol. 76, 35-58. Newport RI: Naval War College 2002.

Lamb, Christopher J. "Information Operations as a Core Competency," Joint Forces Quarterly (December 2004): Iss. 36; pg. 88.

Miller, Michael G. "Information Operations Planning for 2000 and Beyond: The Joint IO Planning Process and IO Navigator." Cyber Sword, (Spring 2000):Vol. 4, no.1, pg.10-13.

Naval War College, Joint Military Operations Department, ISR and Information Operations in Iraqi Freedom-2003, Newport, RI: 19 August 2004

Paschall, Joseph P. "Tactical Information Operations in Iraqi Freedom." Marine Corps Gazette (Mar 2004): Vol. 88, Iss. 3; pg.56.

Shaw, John. "Does the JFC Need a JIOTF? Strengthening IO Doctrine." Cyber Sword, (Fall 1999): Vol. 3, Iss. 1. pg. 4-6.

Scales, Robert MGEN & Cebrowski., Art VADM. "Transformation." Armed Forces Journal, Defense News Media Group. (Mar 2005): Reprint Newport RI; Naval War College, Mar 2005.

Simon, Herbert A., "Decision Making and Problem Solving." Report of the Research Briefing Panel on Decision Making and Problem Solving 1986. National Academy of Sciences. National Academy Press, Washington, DC: 1986. on-line at < http://dieoff.org/page163.htm > [3 May 05]

U.S. Joint Chiefs of Staff. Doctrine for Public Affairs in Joint Operations, Joint Publication 3-61. Washington DC: 04 May 97.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington DC: 09 Oct 98.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations (Second Draft). Joint Publication 3-13. Washington DC: 14 Dec 2004.

U.S. Joint Chiefs of Staff. Doctrine for Joint Psychological Operations. Joint Publication 3-53 Washington DC: 10 July 96.

U.S. Joint Chiefs of Staff. Joint Vision 2020. Washington, DC: June 2000.